We claim:

1. A system for controlling data communication in an ad-hoc network that connects a wireless device and a nearby wireless device, comprising:

a memory device; and

a processor disposed in communication with the memory device, the processor configured to:

store an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters;

determine a priority for each entry in the application directory;

identify a selected entry based on the priority;

examine the attributes and the security parameters for the selected entry; and

establish a security association to support the data communication when the security parameters direct the selected entry to use a secure connection.

2. The system of claim 1, wherein the processor is further configured to:

receive a connection request from the nearby wireless device; and

send a first application directory to the nearby wireless device;

receive a second application directory from the nearby wireless device; and

create the application directory by combining the first application directory and the second application directory.

3. The system of claim 1, wherein the attributes include a device identifier, a role, and control

parameters.

4. The system of claim 3, wherein the control parameters include an application state, and at least one user-defined application setting.

5. The system of claim 1, wherein a bit-string includes the security parameters, a value of the bit-string representing each of the security parameters.

6. The system of claim 1, wherein the security parameters include an information security objective, a cryptography method for attaining the information security objective, and a level of security.

7. The system of claim 6, wherein the information security objective includes maintaining confidentiality, ensuring integrity, authenticating a party, and protecting against replay or reuse.

8. The system of claim 6, wherein the cryptography method includes a signature verification service, and an encryption algorithm.

9. The system of claim 6, wherein the level of security is a minimum required level of security.

10. The system of claim 1, wherein to determine the priority for each entry, the processor is further configured to:

compare the attributes for each entry in said at least one entry.

11. The system of claim 1, wherein to establish the security association, the processor is further configured to:

query a database for an existing security association between the wireless device and the nearby wireless device that will satisfy the security parameters;

reuse the existing security association when the query of the database is successful; and

create a new security association when the query of the database is unsuccessful.

12. The system of claim 11, wherein the processor is further configured to:

store the new security association in a connection log,

wherein the query of the database includes examination of the connection log.

13. The system of claim 11, wherein to reuse the existing security association, the processor is further configured to:

notify the wireless device of the existing security association;

notify the nearby wireless device of the existing security association;

launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

communicate over the secure connection with a counterpart application program on the nearby wireless device.

14. The system of claim 11, wherein to create the new security association, the processor is further configured to:

update the priority of the selected entry to defer the creating of the new security association.

15. The system of claim 11, wherein to create the new security association, the processor is further configured to:

establish a privileged side channel to the nearby wireless device;

negotiate the new security association over the privileged side channel; and

store the new security association.

16. The system of claim 15, wherein the privileged side channel includes a proximity-based communication means, including an infrared data association port, or a direct connection.

17. The system of claim 15, wherein to negotiate the new security association, the processor is further configured to:

send authentication data to the nearby wireless device;

receive counterpart authentication data from the nearby wireless device; and

generate the new security association based on the authentication data and the counterpart authentication data.

18. The system of claim 1, wherein when the security parameters direct the selected entry to use

a non-secure connection, the processor is further configured to:

notify the wireless device of the non-secure connection;

notify the nearby wireless device of the non-secure connection;

launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

communicate over the non-secure connection with a counterpart application program on the nearby wireless device.

19. The system of claim 1, wherein the wireless device initiates the data communication.

20. The system of claim 1, wherein the wireless device stores the application directory.

21. A method for controlling data communication in an ad-hoc network that connects a wireless device and a nearby wireless device, comprising:

storing an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters;

determining a priority for each entry in the application directory;

identifying a selected entry based on the priority;

examining the attributes and the security parameters for the selected entry; and

establishing a security association to support the data communication when the security parameters direct the selected entry to use a secure connection.

22. The method of claim 21, further comprising:

receiving a connection request from the nearby wireless device; and

sending a first application directory to the nearby wireless device;

receiving a second application directory from the nearby wireless device; and

creating the application directory by combining the first application directory and the second application directory.

23. The method of claim 21, wherein the attributes include a device identifier, a role, and control parameters.

24. The method of claim 23, wherein the control parameters include an application state, and at least one user-defined application setting.

25. The method of claim 21, wherein a bit-string includes the security parameters, a value of the bit-string representing each of the security parameters.

26. The method of claim 21, wherein the security parameters include an information security objective, a cryptography method for attaining the information security objective, and a level of security.

27. The method of claim 26, wherein the information security objective includes maintaining

confidentiality, ensuring integrity, authenticating a party, and protecting against replay or reuse.

28. The method of claim 26, wherein the cryptography method includes a signature verification service, and an encryption algorithm.

29. The method of claim 26, wherein the level of security is a minimum required level of security.

30. The method of claim 21, wherein the determining of the priority for each entry further comprises:

comparing the attributes for each entry in said at least one entry.

31. The method of claim 21, wherein the establishing of the security association further comprises:

querying a database for an existing security association between the wireless device and the nearby wireless device that will satisfy the security parameters;

reusing the existing security association when the query of the database is successful; and

creating a new security association when the query of the database is unsuccessful.

32. The method of claim 31, further comprising:

storing the new security association in a connection log,

wherein the query of the database includes examination of the connection log.

33. The method of claim 31, wherein the reusing of the existing security association further comprises:

notifying the wireless device of the existing security association;

notifying the nearby wireless device of the existing security association;

launching an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

communicating over the secure connection with a counterpart application program on the nearby wireless device.

34. The method of claim 31, wherein the creating of the new security association further comprises:

updating the priority of the selected entry to defer the creating of the new security association.

35. The method of claim 31, wherein the creating of the new security association further comprises:

establishing a privileged side channel to the nearby wireless device;

negotiating the new security association over the privileged side channel; and

storing the new security association.

36. The method of claim 35, wherein the privileged side channel includes a proximity-based communication means, including an infrared data association port, or a direct connection.

37. The method of claim 35, wherein the negotiating of the new security association further comprises:

sending authentication data to the nearby wireless device;

receiving counterpart authentication data from the nearby wireless device; and

generating the new security association based on the authentication data and the counterpart authentication data.

38. The method of claim 21, wherein when the security parameters direct the selected entry to use a non-secure connection, the method further comprises:

notifying the wireless device of the non-secure connection;

notifying the nearby wireless device of the non-secure connection;

launching an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

communicating over the non-secure connection with a counterpart application program on the nearby wireless device.

39. The method of claim 21, wherein the wireless device initiates the data communication.

40. The method of claim 21, wherein the wireless device stores the application directory.

41. A computer program product, tangibly stored on a computer-readable medium, for controlling data communication in an ad-hoc network that connects a wireless device and a nearby wireless device, comprising instructions operable to cause a programmable processor to:

store an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters;

determine a priority for each entry in the application directory;

identify a selected entry based on the priority;

examine the attributes and the security parameters for the selected entry; and

establish a security association to support the data communication when the security parameters direct the selected entry to use a secure connection.

42. The computer program product of claim 41, further comprising instructions operable to cause the programmable processor to:

receive a connection request from the nearby wireless device; and

send a first application directory to the nearby wireless device;

receive a second application directory from the nearby wireless device; and

create the application directory by combining the first application directory and the second application directory.

43. The computer program product of claim 41, further comprising instructions operable to

cause the programmable processor to:

compare the attributes for each entry in said at least one entry.

44. The computer program product of claim 41, further comprising instructions operable to cause the programmable processor to:

query a database for an existing security association between the wireless device and the nearby wireless device that will satisfy the security parameters;

reuse the existing security association when the query of the database is successful; and

create a new security association when the query of the database is unsuccessful.

45. The computer program product of claim 44, further comprising instructions operable to cause the programmable processor to:

store the new security association in a connection log,

wherein the query of the database includes examination of the connection log.

46. The computer program product of claim 44, further comprising instructions operable to cause the programmable processor to:

notify the wireless device of the existing security association;

notify the nearby wireless device of the existing security association;

launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

communicate over the secure connection with a counterpart application program on the nearby wireless device.

47. The computer program product of claim 44, further comprising instructions operable to cause the programmable processor to:

update the priority of the selected entry to defer the creating of the new security association.

48. The computer program product of claim 44, further comprising instructions operable to cause the programmable processor to:

establish a privileged side channel to the nearby wireless device;

negotiate the new security association over the privileged side channel; and

store the new security association.

49. The computer program product of claim 48, further comprising instructions operable to cause the programmable processor to:

send authentication data to the nearby wireless device;

receive counterpart authentication data from the nearby wireless device; and

generate the new security association based on the authentication data and the counterpart authentication data.

50. The computer program product of claim 41, wherein when the security parameters direct the selected entry to use a non-secure connection, the computer program product further comprises

instructions operable to cause the programmable processor to:

notify the wireless device of the non-secure connection;

notify the nearby wireless device of the non-secure connection;

launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

communicate over the non-secure connection with a counterpart application program on the nearby wireless device.

51. A system for controlling data communication in an ad-hoc network that connects a wireless device and a nearby wireless device, comprising:

means for storing an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters;

means for determining a priority for each entry in the application directory;

means for identifying a selected entry based on the priority;

means for examining the attributes and the security parameters for the selected entry; and

means for establishing a security association to support the data communication when the security parameters direct the selected entry to use a secure connection.

52. The system of claim 51, further comprising:

means for receiving a connection request from the nearby wireless device; and

means for sending a first application directory to the nearby wireless device;

means for receiving a second application directory from the nearby wireless device; and

means for creating the application directory by combining the first application directory and the second application directory.

53. The system of claim 51, wherein the determining of the priority for each entry further comprises:

means for comparing the attributes for each entry in said at least one entry.

54. The system of claim 51, wherein the means for the establishing of the security association further comprises:

means for querying a database for an existing security association between the wireless device and the nearby wireless device that will satisfy the security parameters;

means for reusing the existing security association when the query of the database is successful; and

means for creating a new security association when the query of the database is unsuccessful.

55. The system of claim 54, further comprising:

means for storing the new security association in a connection log,

wherein the query of the database includes examination of the connection log.

56. The system of claim 54, wherein the means for the reusing of the existing security

association further comprises:

means for notifying the wireless device of the existing security association;

means for notifying the nearby wireless device of the existing security association;

means for launching an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

means for communicating over the secure connection with a counterpart application program on the nearby wireless device.

57. The system of claim 54, wherein the means for the creating of the new security association further comprises:

means for updating the priority of the selected entry to defer the creating of the new security association.

58. The system of claim 54, wherein the means for the creating of the new security association further comprises:

means for establishing a privileged side channel to the nearby wireless device;

means for negotiating the new security association over the privileged side channel; and

means for storing the new security association.

59. The system of claim 58, wherein the means for the negotiating of the new security

association further comprises:

means for sending authentication data to the nearby wireless device;

means for receiving counterpart authentication data from the nearby wireless device; and

means for generating the new security association based on the authentication data and the counterpart authentication data.

60. The system of claim 51, wherein when the security parameters direct the selected entry to use a non-secure connection, further comprising:

means for notifying the wireless device of the non-secure connection;

means for notifying the nearby wireless device of the non-secure connection;

means for launching an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program; and

means for communicating over the non-secure connection with a counterpart application program on the nearby wireless device.

61. A system for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising:

a memory device; and

a processor disposed in communication with the memory device, the processor configured to:

store a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter;

store a copy of the security association;

remove the security association when the first encounter terminates; and

establish a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter.

62. The system of claim 61, wherein the storing of the security association is to a short-term storage device.

63. The system of claim 61, wherein the storing of the copy of the security association is to a long-term storage device.

64. The system of claim 61, wherein to establish the secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for the second encounter, the processor is further configured to:

search a connection log to locate the copy of the security association;

launch the application program associated with the copy of the security association;

configure the secure connection using the security parameters associated with the copy of the security association; and

communicate over the secure connection with the counterpart application program.

65. The system of claim 64, wherein the processor is further configured to:

verify that the copy of the security association will satisfy the security parameters for the second encounter.

66. The system of claim 64, wherein to search the connection log to locate the copy of the security association, the processor is further configured to:

retrieve at least one previous connection from the connection log; and

identify one of said at least one previous connection as the copy of the security association.

67. A method for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising:

storing a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter;

storing a copy of the security association;

removing the security association when the first encounter terminates; and

establishing a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter.

68. The method of claim 67, wherein the storing of the security association is to a short-term storage device.

69. The method of claim 67, wherein the storing of the copy of the security association is to a long-term storage device.

70. The method of claim 67, wherein the establishing of the secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for the second encounter further comprises:

searching a connection log to locate the copy of the security association;

launching the application program associated with the copy of the security association;

configuring the secure connection using the security parameters associated with the copy of the security association; and

communicating over the secure connection with the counterpart application program.

71. The method of claim 70, further comprising:

verifying that the copy of the security association will satisfy the security parameters for the

second encounter.

72. The method of claim 70, wherein the searching of the connection log to locate the copy of the security association further comprises:

retrieving at least one previous connection from the connection log; and

identifying one of said at least one previous connection as the copy of the security association.

73. A computer program product, tangibly stored on a computer-readable medium, for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising instructions operable to cause a programmable processor to:

store a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter;

store a copy of the security association;

remove the security association when the first encounter terminates; and

establish a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter.

74. The computer program product of claim 73, further comprising instructions operable to cause the programmable processor to:

search a connection log to locate the copy of the security association;

launch the application program associated with the copy of the security association;

configure the secure connection using the security parameters associated with the copy of the security association; and

communicate over the secure connection with the counterpart application program.

75. The computer program product of claim 74, further comprising instructions operable to cause the programmable processor to:

verify that the copy of the security association will satisfy the security parameters for the second encounter.

76. The computer program product of claim 74, further comprising instructions operable to cause the programmable processor to:

retrieve at least one previous connection from the connection log; and

identify one of said at least one previous connection as the copy of the security association.

77. A system for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program

identifier, attributes, and security parameters, comprising:

means for storing a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter;

means for storing a copy of the security association;

means for removing the security association when the first encounter terminates; and

means for establishing a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter.

78. The system of claim 77, wherein the means for establishing the secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for the second encounter further comprises:

means for searching a connection log to locate the copy of the security association;

means for launching the application program associated with the copy of the security association;

means for configuring the secure connection using the security parameters associated with the copy of the security association; and

means for communicating over the secure connection with the counterpart application program.

79. The system of claim 78, further comprising:

means for verifying that the copy of the security association will satisfy the security parameters for the second encounter.

80. The system of claim 78, wherein the means for searching the connection log to locate the copy of the security association further comprises:

means for retrieving at least one previous connection from the connection log; and

means for identifying one of said at least one previous connection as the copy of the security association.

81. A graphical user interface for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising:

a first region of a video display connected to the wireless device, the first region including a display list storing at least one previous connection between the wireless device and the nearby wireless device,

wherein a user operates an input device connected to the wireless device to identify one of said at least one previous connection as a selected previous connection, and

wherein the user operates the input device connected to the wireless device to launch the application program associated with the selected previous connection, configure the secure connection using the security parameters associated with the selected

previous connection, and communicate over the secure connection with the counterpart application program.

82. The graphical user interface of claim 81, wherein a memory connected to the wireless device stores a connection log that includes connection data, and wherein the connection data populates the display list.

83. The graphical user interface of claim 81, wherein to identify one of said at least at least one previous connection as the selected previous connection, the user selects an item in the display list by highlighting the item, displaying the item in reverse video, or displaying the item in a different font type, font size, or font style.

84. The graphical user interface of claim 81, wherein the user verifies that the selected previous connection is a copy of the entry.